**Due to the significant volume of recruitment being undertaken by Joint Force Training Centre (JFTC) the processing time for applications will take longer than normal. Once you have submitted your application please ensure that you have received a TALEO/NTAP acknowledgement email, which is your proof that your application has been submitted. After this you will be contacted in due course by our recruitment team with further information on the status of your application, but please note that this may not be for several weeks after the vacancy notice closes.**

3rd NATO Signal Battalion VACANCY NOTICE

Job Number: **240499**

Technician (Cyber Defence)

Applications are now invited for the position of **Technician (Cyber Defence)**, at the 3rd NATO Signal Battalion located in Bydgoszcz, Poland. NATO grade G10. Applications must be made on line (please type Job Number 240499):

https://nato.taleo.net/careersection/2/jobsearch.ftl?lang=en

**Closing Date** for applications: **21 April 2024**

**Location:** Bydgoszcz, Poland

- **Notes for candidates:** The candidature of NATO redundant staff at grade G10 will be considered before any other candidates.

  Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

- **Notes for NATO Civilian Human Resources Managers:** if you have qualified redundant staff at grade G10, please advise JFTC Civilian Human Resources Manager no later than the closing date.

**Contract:** Serving NATO International Civilian staff will be offered a contract in accordance with the NATO Civilian Personnel Regulations. Newly recruited staff will be offered a three year definite duration contract.

**Salary:** Starting basic salary (effective 01 January 2024) is **15,492.60 PLN** per month (tax-free). Additional allowances may apply depending on the personal circumstances of the successful candidate. For further details see *NATO Terms & Conditions of Employment* on the JFTC internet website: www.jftc.nato.int .

For any queries, please contact the JFTC Recruitment Team at: civ.recruitment@jftc.nato.int

If you are an experienced Cyber Defence Technician, looking to join a dynamic team working in a multi-national environment, 3rd NATO Signal Battalion would be interested in hearing from you.

**Post Context**

NATO Signal Battalion operates, maintains, and sustains Deployable Communication Information Systems (DCIS) to enable command and control (C2) in support of deployed NATO Headquarters and entities during Alliance operations, missions and exercises.

The Maintenance and Support Company (M&S Coy) is responsible for Level 1 and Level 2 CIS support of NATO DCIS and for Level 1 and Level 2 preventive and corrective maintenance of non-CIS equipment. Additionally provides all supply related activities and accountability of properties assigned to the NSB.

The Communications and Information Systems Platoon is responsible for Communications and Information Systems (CIS) level 2/2+ CIS support of all Communications and Information Systems (CIS) assets integral to the Battalion. It supervises training, maintenance, and planning of deployable CIS resources in support of Deployable Communication Modules (DCM).

The Mobile Communications, Information Systems and Cyber Defence Section (CIS&CD) is responsible for maintaining and repairing cyber protection systems in support of NSB information system functions. It acts as the planning and standards authority for all cyber activities in support of NATO operations and exercises. It maintains a system of continuous education and training to maintain an up-to-date knowledge of the current NATO cyber defence and CIS systems.

The incumbent is responsible for the protection of classified/unclassified NATO Deployed CIS (DCIS) from Cyberspace threats.

**Reports to:** - Section Head (Mobile Communications, Information Systems and Cyber Defence) - OR-8

**Principal Duties:** He/she will

1. Identifying system vulnerabilities and possible threats and then applying the necessary safeguards (both technical and administrative) to minimize those vulnerabilities and defend against potential attacks.

2. Performing routine system and network monitoring and detecting security incidents or bad security practices that may lead to system compromise.

3. Mentoring and providing on-the-job training to the military Cyber Defence technicians of the M&S Coy Mob CIS and Cyber Defence section.

4. Providing mentoring and technical guidance to the NSB DCMs IS technicians for vulnerability resolution and mitigation.

5. Supporting and guiding the daily Cyber hygiene duties and vulnerability remediation priorities of the military Cyber Defence technicians in accordance with the NCISG Vulnerability Management SOPs and CD engineer directions.

6. Provides Level 2 Cyber Defense support to Deployed CIS.

7. Supporting Defensive Cyberspace Operations (DCO) during operations and exercises, while working at the DCIS Support Group (DSG) and in coordination with the NCISG HQ Cyber Defence engineers.

8. Supporting and guiding the incident response actions of the military Cyber Defence technicians deployed forward in support of operations and exercises in accordance with the NCISG Incident Response SOPs and CD engineer directions.

9. Investigating security incidents and, in coordination with the NSB HQ S-2/6 and NATO CIS Group HQ, supporting appropriate actions.

10. Developing, implementing and disseminating security awareness material and training for supported users in coordination with the NSB HQ S-2 and NATO CIS Group HQ.

11. Assisting the resolution of technically challenging problems with the cyber defence services installed in the deployable networks and systems.

12. Supporting Cyber Defense system installation, configuration and accreditation processes.

13. Participates in meetings, workgroups and projects with different NATO stakeholders as NSB Cyber Defence SME.

14. Supporting NSB Engineering Cell, NCISG J2/6 and NATO CyOC, within own AoR,

**Special Requirements and Additional Duties**

The employee may be required to perform a similar range of duties elsewhere within the organisation at the same grade without there being any change to the contract

Mandatory Deployment Post. - The incumbent may be required to undertake deployments in support of military operations and exercises, and/or TDY assignments, both within and outside NATO boundaries. Such operational deployment may exceed 30 days duration up to 183 days in any period of 547 days, and may be on short notice. For NATO International Civilian Staff, acceptance of an employment contract linked to this post constitutes agreement to deploy in excess of 30 days if required.

The work is normally performed in a Normal NATO office working environment.

Normal Working Conditions apply.

The risk of injury is categorised as No Risk / Risk might increase when deployed.

**Essential Qualifications**

Higher Secondary education and intermediate vocational training in computer science, engineering disciplines, statistics or similar numerate discipline, operations research. or related discipline which might lead to a formal qualification with 2 years experience, or Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 4 years post related experience.

1. Two years of demonstrable experience in the administration of Microsoft Workstation and Server systems, including the management of Active Directory Domains, Group Policy objects and use of the PowerShell console.

2. One year of demonstrable experience in UNIX/LINUX environments.

3. At least 2 years of experience supporting the security of Computer Systems and networks, either as a security-focused administrator or as a member of a Security Operations Center (SOC).

4. Deep knowledge and understanding of TCP/IP stacks, protocols, and ports.

5. Work experience in the use of computer security tools and vulnerability assessment methodologies.

6. Comprehensive knowledge of the principles of computer and communications security, networking, and the vulnerabilities of modern operating systems and applications.

7. General certification in Information Assurance or CIS security (Security+, CCNA Security, GSEC, CEH, CISSP or equivalent).

**Language**

English - SLP 2222 - (Listening, Speaking, Reading and Writing)

NOTE: The work both oral and written in this post and in this Headquarters as a whole is conducted mainly in English.

**Desirable Qualifications**

**a. Professional Experience**

1. Two years of work experience auditing computer systems, network infrastructure, web applications and applications.

2. Work experience in managing and configuring network equipment, firewalls, Intrusion Detection Systems and proxy servers.

3. Work experience with endpoint security and anti-malware management solutions (preferably the Trellix ePO management suite).

4. Work experience with SIEM applications (preferably Splunk).

5. Experience providing support and training to junior technical staff.

6. Experience in Vulnerability Assessment solutions and tools (Tenable.sc, Nessus, or equivalent).

**b. Education/Training**

1. Professional certification in the administration of Microsoft Windows or Linux operating systems (MCSA, RHCSA, Server+ or equivalent).

2. Professional certification in networking (CCNA, CCNP or equivalent).

**Work Environment**

He/she will be required to work in a normal NATO office environment.

Normal Working Conditions apply.

The risk of injury is categorised as No Risk / Risk might increase when deployed.